IN THE SPECIFICATION

Please amend the paragraph on page 3, line 7, as follows:

"The Digital Transmission Content Specification or DTCP ~~(available through the Internet at http://www.dtcp.com)~~ discloses a cryptographic protocol for protecting audio/video (A/V) content from unauthorized copying as it traverses digital transmission mechanisms from device to device. Only compliant devices manufactured to support the DTCP protocol are capable of transmitting or receiving the protected A/V content. Each device is manufactured with a unique device ID and a public/private key pair which facilitate authentication and encryption/decryption of the A/V content. When a source device receives a request to transmit protected A/V content to a sink device, the source and sink devices engage in an authentication transaction. If the authentication transaction is successful, the source device generates an exchange key which is communicated to the sink device. The exchange key is used by the sink device to generate a content key associated with each A/V stream which is used to decrypt the A/V stream."

Please amend the paragraph on page 6, line 8, as follows:

"FIG. 2 shows a secure disk drive 20 according to an embodiment of the present invention as comprising a disk 22 for storing data, and an input 24 for receiving an encrypted message 26 from a client disk drive, the encrypted message 26 comprising ciphertext data and a client drive ID identifying the client disk drive. The secure disk drive 20 comprises a secure drive key 34 and an internal drive ID 38. A key generator 30 within the secure disk drive 20 generates a client drive key 32 based on the client drive ID and the secure drive key 34, and an internal drive key 36 based on the internal drive ID 38 and the secure drive key 34. The secure disk drive 20 further comprises an

authenticator 56 for verifying the authenticity of the encrypted message 26 and generating an enable signal 50, the authenticator 56 is responsive to the encrypted message 26 and the client drive key 32. The secure disk drive further comprises a data processor 40 comprising a message input 42 for receiving the encrypted message 26 from the client disk drive, and a ~~data output 58~~ data output 44 for outputting the ciphertext data 46 to be written to the disk 22. The data processor 40 further comprises an enable input 48 for receiving the enable signal 50 for enabling the data processor 40, and a key input 51 for receiving the internal drive key 36, the internal drive key 36 for use in generating a message authentication code. The data processor 40 outputs reply data 54 comprising the message authentication code. The secure disk drive 20 outputs a reply 60 to the client disk drive, the reply 60 comprising the reply data 54 and the internal drive ID 38."